Adversarial Risk Analysis for Enhancing Combat Simulation Models

Presentation of full paper for ISMS Annual Conference 2015

Juho Roponen, Ahti Salo

About me

- Recent MSc (technology) graduate from Aalto University
- Have been involved in projects focusing on military combat modeling for about 2 years
- Research interests include in no specific order:
  - Physical modeling of effects of weapons
  - Risk analysis approach to combat modeling
  - Tactics in complex games

E-mail juho.roponen@gmail.com

This presentation

1. Introduction
2. What is adversarial risk analysis and why should you care?
3. Possible uses in context of combat simulation models
4. Example case
5. Questions and answers

Adversarial Risk Analysis (ARA)

- Combines statistical risk analysis with game theory
- Suitable for analyzing situations where two or more intelligent actors with conflicting interests make decisions under uncertain outcomes
- Current uses include, for example, counter-terrorism and corporate finance

Why is ARA interesting in the context of military combat models?

- Originally developed for counter-terrorism
  - Well suited for representing two hostile actors
  - Has not been applied to combat simulation models yet
- Generic enought to be applicable to wide variety of problems
- Overcomes many problems that are present with game theory solutions
  - Can represent opponents that do not adhere to minmax rationality princible
  - No need to assume the actors share some common knowledge

Possible uses – Simulating chains of events

- Usually requires compromise between scale and amount of detail
- Has already been done using methods of probabilistic risk analysis
- The methodology can be used with many different simulation tools
- Potentially useful in data farming

Modeling the effects of military deceit

- Difficult to predict and simulate using existing software
  - Often relies only on user's expert opinion
- Commonly used solution is wargaming which has its own problems
  - Decisions in a game do not always correspond with decisions in the real world
  - Often captures typical decision making instead of optimal decision making
- ARA methodology can be used to complement these expert opinion approaches
- ARA makes it very easy to model cases in which the adversary is fed misinformation about strength of opposing forces

Other possible usage cases

- Distribution of resources
- Modeling decision making
- Supporting decision making

Limitations of ARA

- Decisions modeled need to be quantifiable
- Number of possible choices needs to be limited
- Length of decision chains needs to be limited
- Can only predict the outcomes of decisions if the decision-maker’s logic is known

Example case

- Two adversaries: the Defender and the Attacker
- The Defender has two targets he wants to protect
  - 40 soldiers at the first target
  - 20 soldiers at the second target
- The Attacker can choose which target to attack
- The Defender has the option of moving soldiers secretly between the targets before the Attacker has a chance to act
- There is a chance the Attacker will find out about the troop movement, but if he doesn’t he will be acting on incomplete information

Influence diagram from the Defender’s point of view

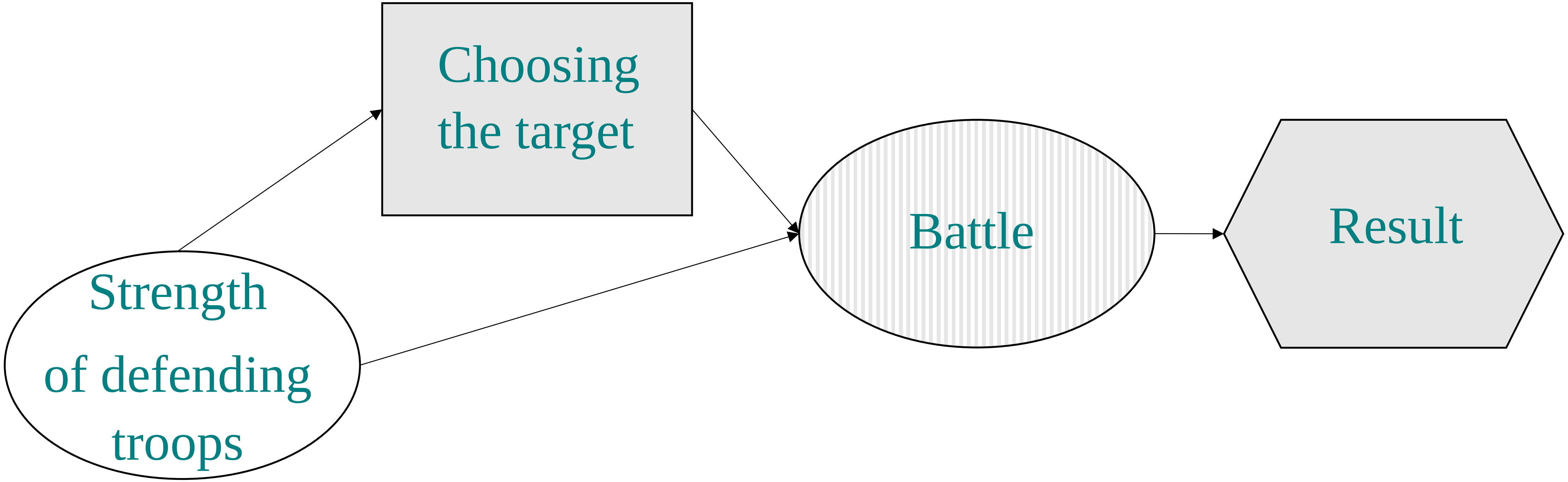
Example case from the Defender’s point of view

- Attacker is assumed a utility maximizer
- The expected utility gained from the attack by the Attacker is

$$\psi_A(a,d,R) = p_A(S=0|a,d,R)\sum_{c_A}\sum_{c_D}[u_A(c_A,c_D)\pi_A(c_A,c_D|a,d,R,S=0)]$$
$$+\,p_A(S=1|a,d,R)\sum_{c_A}\sum_{c_D}[u_A(c_A,c_D)\pi_A(c_A,c_D|a,d,R,S=1)].$$

- The Defender’s expected utility is similar

Influence diagram from the Attacker’s point of view



The Defender’s utility function

- The Defender considers target 1 twice as valuable as target 2
- Specifically he assesses that the utility gained (in this case lost) from the attack is

$$u_D(S, a, c_A, c_D) = -40(2-a)(1-S) - 20(a-1)(1-S) + 0.1c_A - c_D$$

- It is not enough for the Defender to know the utilities gained from all the possible combinations of choices and chance if he does not know what the Attacker will choose

Defender's estimations on troop strengths

- The Attacker has at least 20 men but no more than 35, and the Defender thinks that the most likely number is 30, so he fits a triangular distribution.
- The Attacker thinks the Defender has 36 to 44 men at Target 1 and 18 to 22 men at Target 2 (with all values equally probable).
- The Attacker has probability $p_R = 0.1$ of finding out about the Defender's troop movement.

The Attacker's utility function

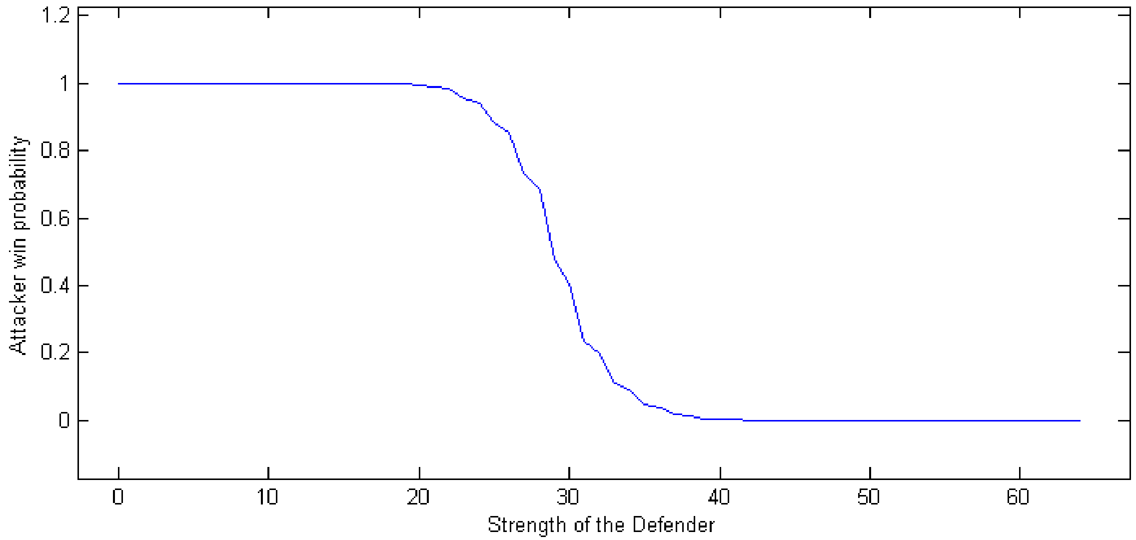
- The Defender needs to estimate the Attacker's utility function as well
- He estimates that it is similar to his own, but is not certain that the Attacker places the exact same value on the targets

$$u_A(S, a, c_A, c_D) = (40 + u_1)(2 - a)(1 - S) + (20 + u_2)(a - 1)(1 - S) + 0.1c_D - c_A$$

- u_1 and u_1 were assumed to follow uniform distribution to make calculations simpler

Solving the problem step by step

1. Calculate the success probabilities and expected losses for both sides for all the possible combinations of strengths of both sides as perceived by the attacker taking into account the fact that the Attacker detects the Defender's troop movement on probability p_R.



Solving the problem step by step

2. Calculate the Attacker's expected utilities ψ_A for attacking and not attacking for all possible strengths of the Attacker's force taking into account the uncertainties with u_A.

3. Compare the expected utilities to get an estimate for the probability of an attack on each target for each possible strength of the Attacker.

Solving the problem step by step

4. Consider the probability of an attack with a specific strength of the attacker and the probability for each of those strengths to calculate $p_D(a|d,R)$.

5. Calculate ψ_D for all possible values of a.

6. Use $p_D(a|d,R)$ to determine the decision *d* which maxizes his expected utility.

Execution and results

- A lightweight simulation model capable of calculating duels between two forces was used
- The step by step algorithm was made into program code
- The maximum utility gained by the Defender was -6.7
- The optimal choice was to move 18 soldiers from target 1 to target 2

Recap

1. Adversarial risk analysis (ARA) is a methodology for estimating the actions of a rational adversary
2. It can be used for some combat modeling problems that are difficult or impossible to solve otherwise
3. It’s a very good tool estimating the effectiveness of military deceit

Questions?

E-mail juho.roponen@gmail.com